

On the Expressive Power of Kleene Algebra with Domain

Georg Struth
University of Sheffield, UK

Abstract

It is shown that antidomain semirings are more expressive than test semirings and that Kleene algebras with domain are more expressive than Kleene algebras with tests. It is also shown that Kleene algebras with domain are expressive for propositional Hoare logic whereas Kleene algebras with tests are not.

1 Introduction

Kleene algebras with tests (KAT) [4] yield arguably the simplest and most elegant model of the control flow in simple while-programs. They provide an abstract algebraic view on the standard relational semantics of imperative programs, have been applied to various program analysis tasks and form the backbone of program construction and verification tools. In particular, the inference rules of propositional Hoare logic (PHL)—Hoare logic without assignment rule—can be derived in this setting [5]. Kleene algebras with domain (KAD) [1, 3] are a similar formalism that provides an algebraic approach to propositional dynamic logic and predicate transformer semantics. The inference rules of PHL are derivable in KAD as well and it is known that every KAD is a KAT [3].

From a complexity point of view, the equational theory of KAT is known to be PSPACE complete [6], whereas that of KAD is decidable in EXPTIME [7]. It seems also plausible that KAD is more expressive than KAT; after all, image and preimage as well as modal box and diamond operators can be defined in the former algebra.

This article makes this gap in expressive power precise, showing that KAD is strictly more expressive than KAT with a simple, natural and interesting example. Firstly it is shown that the inverse of the sequential composition rule of PHL, when expressed as a formula in the language of KAT, is derivable from the axioms of KAD. Secondly, a model of KAT is presented in which this formula does not hold. In addition it is shown that KAT is not expressive for PHL, whereas this is trivially the case for KAD.

Inverting the inference rules of Hoare logic is interesting for verification condition generation in the context of program correctness, where intermediate assertions such as weakest liberal preconditions need to be computed. It is also related to the question of expressivity of Hoare logic in relative completeness proofs.

2 KAD and KAT

A *semiring* is a structure $(S, +, \cdot, 0, 1)$ such that $(S, +, 0)$ is a commutative monoid, $(S, \cdot, 1)$ is a monoid; and the two monoids interact via the distributivity laws $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(x + y) \cdot z = x \cdot z + y \cdot z$ and the annihilation laws $0 \cdot x = 0$ and $x \cdot 0 = 0$.

A *dioid* is an additively idempotent semiring, that is, $x + x = x$ holds for all $x \in S$. In this case, $(S, +)$ forms a semilattice with order relation defined as $x \leq y \Leftrightarrow x + y = y$. Multiplication is isotone with respect to the order, $x \leq y$ implies both $z \cdot x \leq z \cdot y$ and $x \cdot z \leq y \cdot z$, and $0 \leq x$ holds for all $x \in S$.

A *Kleene algebra* is a dioid expanded by a star operation that satisfies the unfold and induction axioms

$$1 + x \cdot x^* = x^*, \quad 1 + x^* \cdot x = x^*, \quad z + x \cdot y \leq y \Rightarrow x^* \cdot z \leq y, \quad z + y \cdot x \leq y \Rightarrow z \cdot x^* \leq y.$$

An *antidomain semiring* [3] is a semiring S endowed with an operation $a : S \rightarrow S$ that satisfies

$$a(x) \cdot x = 0, \quad a(x \cdot y) + a(x \cdot a(y)) = a(x \cdot a(y)), \quad a(x) + a(a(x)) = 1.$$

These axioms imply that every antidomain semiring is a dioid. A *domain operation* can be defined on S as $d = a \circ a$. It is a retraction, that is, $d \circ d = d$, and it follows that $x \in d(S) \Leftrightarrow d(x) = x$, where $d(S)$ denotes the image of the set S under d . This fact can be used to show that $(d(S), +, \cdot, a, 0, 1)$ forms a boolean algebra in which multiplication coincides with meet and the antidomain operator a yields test complementation. In addition we need the following fact about antidomain semirings.

Lemma 1 ([3]). *In every antidomain semiring, $x \cdot y = 0 \Leftrightarrow x \cdot d(y) = 0$.*

A *Kleene algebra with domain* [3] is both a Kleene algebra and an antidomain semiring.

A *test semiring* is a dioid S in which a boolean algebra B is embedded by a map $\iota : B \rightarrow S$ such that

$$\iota(0) = 0, \quad \iota(1) = 1, \quad \iota(x \sqcup y) = \iota(x) + \iota(y), \quad \iota(x \sqcap y) = \iota(x) \cdot \iota(y).$$

A *Kleene algebra with tests* [4] is both a Kleene algebra and a test semiring. In the tradition of Kleene algebras with tests the embedding is left implicit. I write p, q, r, \dots for boolean elements, which are called *tests*, and x, y, z for arbitrary semiring elements. I write AS for the class and axiom system of domain semirings, TS for that of test semirings, KAD for that of Kleene algebras with domain and KAT for that of Kleene algebras with tests.

Lemma 2 ([3]). $\text{KAD} \subseteq \text{KAT}$.

Proof. If $K \in \text{KAD}$ then $d(K)$ is a boolean algebra, hence a test algebra. The embedding is provided by the identity function on $d(K)$ as a subset of K . Thus $K \in \text{KAT}$. \square

It follows that $\text{AS} \subseteq \text{TS}$. Thus, for any $K \in \text{KAD}$, all elements in $d(K)$ may serve as tests in the associated $(K, d(K)) \in \text{KAT}$.

The notions of domain, antidomain and tests can be motivated from the model of binary relations.

Proposition 1 ([5, 3]). *Let $2^{A \times A}$ be the set of binary relations over the set A . Suppose that*

$$\begin{aligned} R \cdot S &= \{(a, b) \mid \exists c. (a, c) \in R \wedge (c, b) \in S\}, & id &= \{(a, a) \mid a \in A\}, \\ a(R) &= \{(a, a) \mid \forall b. (a, b) \notin R\}, & R^* &= \bigcup_{i \in \mathbb{N}} R^i, \end{aligned}$$

where $R^0 = id$ and $R^{i+1} = R \cdot R^i$. Then

1. $(2^{A \times A}, \{R \mid R \subseteq id\}, \cup, \cdot, \emptyset, id, *) \in \text{KAT}$,
2. $(2^{A \times A}, \cup, \cdot, \emptyset, id, a, *) \in \text{KAD}$.

The operation \cdot on relations is the standard relational product; id is the identity relation on S . The operation a is the domain complement on relations; $a(R)$ represents those states in S that are not related by R to any other state.

3 Expressive Power of KAD and Invertibility in PHL

To show that domain semirings are strictly more expressive than test semirings and that Kleene algebras with domain are strictly more expressive than Kleene algebras with tests I display a sentence φ in the language of KAT such that $\text{KAT} \not\models \varphi$ and $\text{KAD} \vdash \varphi$. To prove that $\text{KAT} \not\models \varphi$ I display a $(K, B) \in \text{KAT}$ such that $(K, B) \not\models \varphi$.

The sentence φ chosen for this purpose is related to the relative completeness of Hoare logic. It is well known that the validity of a Hoare triple can be encoded in the language of KAT [5], and hence KAD, as

$$\{p\}x\{q\} \Leftrightarrow p \cdot x \cdot \bar{q} = 0,$$

where tests p and q serve as assertions and \bar{q} represents the boolean complement of test q . Moreover the inference rules of PHL are derivable in KAT [5]. In particular the rule $\{p\}x\{r\} \wedge \{r\}y\{q\} \Rightarrow \{p\}x \cdot y\{q\}$ for sequential composition can be derived in TS and AS. Invertibility of this rule means finding for any Hoare triple $\{p\}x \cdot y\{q\}$ an assertion r such that $\{p\}x\{r\}$ and $\{r\}y\{q\}$. Hence consider the following sentence in the language of KAT:

$$\varphi \equiv (\forall x, y \in K, p \in B, q \in B. \{p\}x \cdot y\{q\} \Rightarrow (\exists r \in B. \{p\}x\{r\} \wedge \{r\}y\{q\})).$$

Lemma 3. KAT $\not\models \varphi$.

Proof. Consider the KAT $(\{a\}, \{0, 1\}, +, \cdot, 0, 1, *)$ with addition defined by $0 \leq a \leq 1$, multiplication by $a \cdot a = 0$ and $a^* = 1$ (all other operations on elements being fixed). Note that a is not a test because $a \cdot a \neq a$. In this algebra, $1 \cdot a \cdot a \cdot \bar{0} = 1 \cdot 0 \cdot 1 = 0$. However, r can neither be 0 or 1. In the first case, $1 \cdot a \cdot \bar{0} = 1 \cdot a \cdot 1 = 1$; in the second one, $1 \cdot a \cdot \bar{0} = 1 \cdot a \cdot 1 = a$. \square

Lemma 4. AS $\vdash \varphi$.

Proof. Let $S \in \text{AS}$ and suppose $p \cdot x \cdot y \cdot \bar{q} = 0$, with $p, q \in d(S)$. We need an expression r such that $p \cdot x \cdot \bar{r} = 0$ and $r \cdot y \cdot \bar{q} = 0$. So let $r = a(y \cdot \bar{q})$. The assumption and Lemma 1 then imply that $p \cdot x \cdot \bar{r} = p \cdot x \cdot d(y \cdot \bar{q}) = 0$. Moreover, $r \cdot y \cdot \bar{q} = a(y \cdot \bar{q}) \cdot y \cdot \bar{q} = 0$ follows from the first antidomain axiom. \square

These two lemmas can be summarised as follows.

Theorem 1. *There exists a sentence in the language of KAT which is derivable from the AS axioms, but not from the KAT axioms.*

Thus antidomain semirings are strictly more expressive than test semirings, and Kleene algebras with domain are strictly more expressive than Kleene algebras with tests.

4 Expressive Power of KAD and Expressivity of PHL

The question of invertibility of the rules of Hoare logic relates to its expressivity, requiring that for each command x and postcondition q the weakest liberal precondition be definable. In any $K \in \text{KAD}$, the weakest liberal precondition exists for any element $x \in K$ and test $p \in d(K)$ by definition.

Formally, for all $x, y \in K$ one can define a modal box operator

$$[x]y = a(x \cdot a(y))$$

and show that $p \leq [x]q \Leftrightarrow p \cdot x \cdot q = 0$. So $\{p\}x\{q\} \Leftrightarrow p \leq [x]q$ yields an alternative definition of the validity of Hoare triples, in which $\lambda p. [x]p : d(K) \rightarrow d(K)$ is a predicate transformer [7].

It follows that $\{[x]q\}x\{q\} \text{---} [x]p$ is a precondition for x and q —and $\{p\}x\{q\} \Rightarrow p \leq [x]q \text{---} [x]p$ is weaker than any other precondition of x and q . Hence $[x]q$ models indeed the weakest liberal precondition of x and q . Since the standard relational semantics of while programs without the assignment rules can be captured in KAT [4] (and KAD) by defining **if** p **then** x **else** $y = p \cdot x + \bar{p} \cdot y$ and **while** p **do** $x = (p \cdot x)^* \cdot \bar{p}$, the following fact is obvious.

Theorem 2. KAD is expressive for PHL.

The proof of Lemma 4 can now be rewritten in the light of this discussion. First of all, $r = [y]q$ models precisely the weakest liberal precondition of y and q . The next Lemma then arises as an instance of φ in combination with the sequential composition rule of Hoare logic.

Lemma 5. $AS \vdash \{p\}x \cdot y\{q\} \Leftrightarrow \{p\}x\{[y]q\}$.

The second, implicit conjunct is of course $\{[x]q\}x\{q\}$. It is valid and has therefore been deleted.

In KAT the situation is different.

Theorem 3. *KAT is not expressive for PHL.*

Proof. Let A be an infinite set and $\mathcal{B} = \{B \subseteq A \mid B \text{ is finite}\} \cup \{B \subseteq A \mid B \text{ is cofinite}\}$. It has been shown that $(2^A, \mathcal{B}, \cup, \cap, \emptyset, S, *) \in \text{KAT}$ in which $B^* = A$ for all $B \subseteq A$ [1]. The test algebra \mathcal{B} is not complete because suprema of infinitely many finite sets need not be in \mathcal{B} .

Consider the set $C \in 2^A - \mathcal{B}$ and suppose that $a(C \cap a(\emptyset)) = a(C \cap A) = a(C)$, the weakest liberal precondition of C and \emptyset , exists. Thus $a(C) \cap C = \emptyset$ by definition. In addition, C has of course a complement $\overline{C} \in A - \mathcal{B}$ as well. It follows that $a(C) \subset \overline{C}$ and hence $\overline{C} - a(C) \neq \emptyset$.

So let $x \in \overline{C} - a(C)$ and consider the set $a(C) \cup \{x\}$. By construction it is an element of \mathcal{B} that contains $a(C)$ and still satisfies $(a(C) \cup \{x\}) \cap C = \emptyset$. This contradicts the maximality assumption on $a(C)$.

Hence there is a KAT in which for some element x and test p the weakest liberal precondition $[x]p$ of x and p does not exist and KAT is not expressive for PHL. \square

5 Concluding Remarks

The left distributivity law $x \cdot (y + z) = x \cdot z + y \cdot z$ is not needed in the proof of Lemma 4 (and Lemma 1). Formula φ can be derived already from the axioms of antidomain near-semirings [2] and Kleene algebras with domain based on near-semirings are already more expressive than KAT.

The result of Lemma 4 can be dualised and extended, so that other solutions for r can be found. A notion of opposition duality can be defined on a semiring by swapping the order of multiplication. Obviously, the opposite of every Kleene algebra is again a Kleene algebra. The domain operation on a semiring translates to a range operation on the opposite semiring, and vice versa [3]. Thus an antirange and a range operation on a semiring can be axiomatised by $x \cdot ar(x) = 0$, $ar(x \cdot y) + ar(r(x) \cdot y) = ar(r(x) \cdot y)$ and $ar(x) + r(x) = 1$. It is then easy to check that $r = r(p \cdot x)$ provides a solution to a dual variant of Lemma 4. The proof uses the fact that $x \cdot y = 0$ is equivalent to $r(x) \cdot y = 0$ in antirange semirings, which is obtained from Lemma 1 by opposition duality.

One can also consider Kleene algebras with antidomain and antirange operations. It is then appropriate to impose $d(ar(x)) = ar(x)$ and $r(a(x)) = a(x)$ to enforce that $d(S)$ and $r(S)$ coincide [3]. In this context, also $r = r(p \cdot x) \cdot a(y \cdot \overline{q})$ provides a third solution to a generalised variant of Lemma 4.

A final remark concerns the invertibility of the remaining inference rules of propositional Hoare logic. Invertibility of the consequence rule(s) is trivial. The equivalence

$$\{p \cdot t\}x\{q\} \wedge \{p \cdot \overline{t}\}y\{q\} \Leftrightarrow \{p\}\text{if } p \text{ then } x \text{ else } y\{q\}$$

is derivable in KAT: that $\{p\}\text{if } p \text{ then } x \text{ else } y\{q\}$ implies $\{p \cdot t\}x\{q\}$, for instance, is verified by

$$0 = t \cdot 0 = t \cdot p \cdot (t \cdot x + \overline{t} \cdot y) \cdot \overline{q} = (p \cdot t \cdot t \cdot x \cdot \overline{q} + p \cdot t \cdot \overline{t} \cdot y \cdot \overline{q}) = p \cdot t \cdot x \cdot \overline{q} + 0 = \{p \cdot t\}x\{q\}.$$

For the while rule $\{p \cdot t\}x\{p\} \Rightarrow \{p\}\text{while } t \text{ do } x\{p \cdot \overline{t}\}$, the stronger consequent $\{p\}(t \cdot x)^*\{p\}$ —the while loop satisfies the invariant p —is derivable from the antecedent, and invertibility follows from

$$p \cdot t \cdot x \cdot \overline{p} \leq p \cdot (t \cdot x)^* \cdot \overline{p} = 0.$$

References

- [1] J. Desharnais, B. Möller, and G. Struth. Kleene algebra with domain. *ACM TOCL.*, 7(4):798–833, 2006.
- [2] J. Desharnais and G. Struth. Domain axioms for a family of near-semirings. In J. Meseguer and G. Rosu, editors, *AMAST 08*, volume 5140 of *LNCs*, pages 330–345. Springer, 2008.

- [3] J. Desharnais and G. Struth. Internal axioms for domain semirings. *Science of Computer Programming*, 76(3):181–203, 2011.
- [4] D. Kozen. Kleene algebra with tests. *ACM TOPLAS*, 19(3):427–443, 1997.
- [5] D. Kozen. On Hoare logic and Kleene algebra with tests. *ACM TOCL*, 1(1):60–76, 2000.
- [6] D. Kozen and F. Smith. Kleene algebra with tests: Completeness and decidability. In D. van Dalen and M. Bezem, editors, *CSL ’96*, volume 1258 of *LNCS*, pages 244–259. Springer, 1997.
- [7] B. Möller and G. Struth. Algebras of modal operators and partial correctness. *Theoretical Computer Science*, 351(2):221–239, 2006.